UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

JOHNNY PATRICK, on behalf of himself and all others similarly situated,

Plaintiff

v.

NORTHWOOD INC.

Defendant.

Case No.:

Hon.

JURY DEMAND

CLASS ACTION COMPLAINT FOR DAMAGES, EQUITABLE, DECLARATORY AND INJUNCTIVE RELIEF

Plaintiff Johnny Patrick ("Plaintiff"), individually, by and through his undersigned counsel, brings this class action lawsuit against Northwood Inc., ("Defendant" or "Northwood"), on behalf of himself and all others similarly situated, and alleges, based upon information and belief and the investigation of his counsel as follows:

INTRODUCTION

1. Northwood is specialized provider of durable medical equipment, prosthetics, orthotics and medical supplies to patient members of a various healthcare plans such as Blue Cross Blue Shield of Michigan, Blue Care, Health New England, and Security Health Plan of Wisconsin among others.

2. On July 12, 2019, Northwood announced that an unauthorized third party had gained unfettered access over a 3 day period to an employee email account which contained the sensitive personally identifiable information and protected health information of patients who received medical equipment and/or services supplied by Northwood (collectively, "PII"). [1] The exposed PII included patient names, dates of birth, medical record numbers, member health plan identification, diagnoses and codes, treatment details, medical device information, Social Security and driver's license numbers ("Data Breach"). The Data Breach affected approximately 15,000 patients.

---

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information 2 CFR § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number, driver's license number, financial account number). Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, ("HIPAA"), protected health information ("PHI") is considered to be individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103. Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

3. Although the Data Breach occurred on May 3, 2019, and was discovered three days later, Northwood took more than two months to notify affected patients, depriving them of the ability to promptly mitigate potential adverse consequences.

4. This Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect patient PII.

5. Defendant disregarded the rights of Plaintiff and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard patient PII; failing to take standard and reasonably available steps to prevent the Data Breach; failing to monitor and timely detect the Data Breach; and failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

6. As a result of Defendant's failure to implement and follow basic security procedures, patient PII is now in the hands of thieves. Plaintiff and Class Members have had to spend, and will continue to spend, significant amounts of time and money in an effort to protect themselves from the adverse ramifications of the Data Breach and will forever be at a heightened risk of identity theft and fraud.

7. Plaintiff, on behalf of all others similarly situated, alleges claims for negligence, invasion of privacy, breach of implied contract, unjust enrichment, breach of fiduciary duty and violation of the Michigan Consumer Protection Act and seeks to compel Defendant to adopt reasonably sufficient security practices to safeguard patient PII that remains in its custody in order to prevent incidents like the Data Breach from reoccurring in the future.

PARTIES

8. Plaintiff Johnny Patrick is a resident of Mio, Michigan and a member of the McLaren Health Plan, through which he received Northwood's services. On or about July 12, 2019, Mr. Patrick received notice from Northwood, along with 15,000 other patients, that his sensitive PII had been improperly exposed to unauthorized third parties.

9. A few weeks after the Data Breach, Mr. Patrick was notified by Experian that multiple fraudulent attempts had been made to obtain loans and/or credit cards using his identity. For example, on or about May 22, 2019, an unauthorized third party attempted to take out a loan in his name with Main Finance. On the same day, an unauthorized third party attempted to use his PII to obtain a credit card with Capital One.

10. Since the announcement of the Data Breach, Mr. Patrick continues to monitor his accounts in an effort to detect and prevent any misuses of his personal information.

11. Mr. Patrick has, and continues to spend his valuable time to protect the integrity of his finances and credit—time which he would not have had to expend but for the Data Breach.

12. Plaintiff suffered actual injury from having his PII stolen as a result of the Data Breach including, but not limited to: (a) paying monies to Northwood for its goods and services which he would not have had if Northwood disclosed that it lacked data security practices adequate to safeguard consumers' PII from theft; (b) damages to and diminution in the value of his PII—a form of intangible property that the Plaintiff entrusted to Northwood as a condition for health related services; (c) loss of his privacy; (d) imminent and impending injury arising from the increased risk of fraud and identity theft.

13. As a result of the Data Breach, Mr. Patrick will continue to be at heightened risk for financial fraud, medical fraud and identity theft, and their attendant damages for years to come.

14. Defendant Northwood, Inc. is a Michigan corporation located at 25790 Commerce Drive, Madison Heights, MI 48071. It was established in 1992 as a specialized network of durable medical equipment, prosthetics, orthotics and

medical supplies providers offering cost-effective, high-quality products to health plans and self-funded groups. In addition to providing durable medical equipment, today Northwood also provides infusion therapy and pharmacy benefit management including home health, home modification, transportation and translation services.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. There are approximately 15,027 putative class members, and at least some members of the proposed Class have a different citizenship from Northwood.

16. This Court has jurisdiction over the Defendant which operates in this District, and the computer systems implicated in this Data Breach are likely based in this District.

17. Plaintiff received services from Northwood and engaged in underlying health services within this District where his PII was also maintained, and where the breach occurred which led to him sustaining damage. Through its business operations in this District, Northwood intentionally avails itself of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

18. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District. Northwood is based in this District, maintains patient PII in the District and has caused harm to Plaintiff and Class members residing in this District.

STATEMENT OF FACTS

A. The Northwood Data Breach

19. On May 6, 2019, Northwood discovered that the PII of 15,027 of its patients had been compromised as a result of a phishing attack. Northwood indicated that a hacker had gained access to the email account of one of its employees to which it had unfettered access for a period of 3 days (May 3, 2019 to May 6, 2019). Northwood claims that it subsequently determined, on June 19, 2019, that the affected email account contained sensitive PII belonging to individuals who received durable medical equipment either supplied or managed by Northwood. The PII included: names, addresses, dates of birth, dates of service, provider names, medical record numbers, patient identification numbers, medical device descriptions, diagnoses, diagnoses codes, treatment information, member health plan identification, Social Security numbers, driver's license numbers and health insurance provider names.

20. Despite becoming aware of the breach on May 6, 2019, Northwood waited 67 days before informing affected patients that their sensitive PII had been compromised.

21. Despite becoming aware of the origination of the breach on June 19, 2019, Northwood waited almost a full month before it informed patients that their sensitive PII had been compromised.

22. On July 12, 2019, Northwood publicly announced the Data Breach stating in relevant part as follows:

> **About the data privacy event**
>
> Northwood, Inc. ("Northwood") recently discovered an incident that may affect the security of personal information of certain individuals, including those who received durable medical equipment either supplied or managed by Northwood. We take this incident very seriously, and we have been working diligently with the assistance of third-party forensic investigators to determine the full nature and scope of this incident. We are taking additional actions to strengthen the security of our email systems moving forward. Northwood is also contacting the appropriate regulators regarding this incident.
>
> What happened? On May 6, 2019, Northwood became aware of suspicious activity relating to an employee email account. We immediately launched an investigation to determine what may have happened and what information may have been affected. Working together with a leading computer forensics expert, our investigation determined that an unauthorized individual or individuals accessed the email account between May 3, 2019 and May 6, 2019. Because Northwood was unable to determine which email messages in the account may have been opened or viewed by the unauthorized actor, we reviewed the contents of the entire email account to identify what personal information was stored within it.

What information may have been affected by this incident?

On June 19, 2019, Northwood determined that the affected email account contained information related to certain individuals who received durable medical equipment either supplied or managed by Northwood. The type of information affected varies per impacted individual, and includes one or more of the following types of information: name, address, date of birth, date(s) of service, provider name, medical record number, patient identification number, medical device description, diagnosis, diagnosis code(s), treatment information, member health plan identification, and in a very small number of instances, Social Security numbers, driver's license number and health insurance provider names were also impacted for healthcare plan members.

Separately, also contained in the impacted email account was information pertaining to certain healthcare providers in connection with their exclusion status with the Centers for Medicare & Medicaid Services, including their names and Social Security numbers.

Although we cannot confirm that any individual's personal information was actually accessed, or viewed without permission, we are providing this notice out of an abundance of caution. While our investigation is ongoing, we do not currently have any evidence of actual or attempted misuse of any individual's information as a result of this incident.

How will individuals know if they are affected by this incident?

Northwood is mailing notice letters to the individuals whose protected information was contained within the affected email account and may have been accessed or acquired by an unauthorized actor. If an individual did not receive a letter but would like to know if they are affected, they may call the hotline listed below.

What is Northwood doing?

Northwood has strict security measures in place to protect the information in out possession. Upon learning of this incident, we immediately took the impacted email account offline and changed the account password. Northwood then implemented mandatory password resets for all employee email accounts and notified employees to be on the lookout for suspicious

> emails. We implemented additional technical safeguards on our email system, as well as training and education for our employees in order to prevent similar future incidents. We are also offering the impacted individuals access to complimentary credit monitoring services as an added precaution. Because Northwood has insufficient contact information for some of the individuals whose information may be contained in the impacted employee email account, we are providing notice to potentially impacted individuals by way of a notification published to certain state media outlets and in certain state media publications. . Northwood is mailing notice letters to those individuals for whom it has confirmed mailing address information. Northwood has reported this incident to law enforcement. Although we are not aware of any actual or attempted misuse of any individuals' information, we are also providing the impacted individuals access to complimentary credit monitoring services as an added precaution.[2]

B. Prevalence of Cyber Attacks and Particular Susceptibility of the Healthcare Sector

23. Cyber-attacks come in many forms. Phishing attacks are among the oldest, most common, and well known. In simple terms, phishing is a method of obtaining personal information using deceptive e-mails and websites. The goal is to trick an e-mail recipient into believing that the message is something they want or need from a legitimate or trustworthy source and to subsequently take and action such as clicking on a link or downloading an attachment. The fake link will typically mimic a familiar website and require the input of credentials. Once input, the credentials are then used to gain unauthorized access into a system. "It's one of the

---

[2] https://www.prnewswire.com/news-releases/northwood-inc-provides-notice-of-data-security-incident-300884252.html.

oldest types of cyber-attacks, dating back to the 1990s" and one that every organization with an internet presence is aware."[3] It remains the "simplest kind of cyberattack and, at the same time, the most dangerous and effective."[4]

24. Phishing attacks are well known and understood by the cyber-protection community and are generally preventable with the implementation of a variety of proactive measures such as sandboxing inbound e-mail[5], inspecting and analyzing web traffic, penetration testing an organization to find weak spots[6], and employee education, among others.

25. In 2016, the number of U.S. data breaches surpassed 1,000, a record high and a forty percent increase in the number of data breaches from the previous

---

[3] https://www.csoonline.com/article/2117843/phishing/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html.

[4] *All About Phishing*, Malwarebytes, https://www.malwarebytes.com/phishing/.

[5] An automated process whereby e-mails with attachments and links are segregated to an isolated test environment, a "sandbox," wherein a suspicious file or URL may be executed safely.

[6] *See*, https://searchsecurity.techtarget.com/definition/penetration-testing (The practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit. The main objective of penetration testing is to identify security weaknesses. Penetration testing can also be used to test an organization's security policy, its adherence to compliance requirements, its employees' security awareness and the organization's ability to identify and respond to security incident. The primary goal of a pen test is to identify weak spots in an organization's security posture, as well as measure the compliance of its security policy, test the staff's awareness of security issues and determine whether -- and how -- the organization would be subject to security disasters.)

year.[7] In 2017 a new record high of 1,579 breaches were reported representing a 44.7 percent increase over 2016.[8]

26. In 2018, the healthcare sector reported the second largest number of breaches among all measured sectors and the highest rate of exposure per breach.[9] Indeed, healthcare related data is among the most sensitive, and personally consequential when compromised. A report focusing on health-care breaches found that the "average total cost to resolve an identity theft-related incident…came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for health care they did not receive in order to restore coverage.[10] Almost 50 percent of the victims lost their health care coverage as a result of the incident, while nearly one-third said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and

---

[7] Identity Theft Resource Center *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), *available at* https://www.idtheftcenter.org/surveys-studys.

[8] Identity Theft Resource Center, 2017 Annual Data Breach Year-End Review, available at https://www.idtheftcenter.org/2017-data-breaches/.

[9] Identity Theft Resource Center, 2018 End -of-Year Data Breach Report. Available at https://www.idtheftcenter.org/2018-data-breaches/.

[10] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March3, 2010) https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims.

identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.[11]

27. Healthcare related data breaches in particular have continued to rapidly increase. According to the 2019 HIMSS Cybersecurity Survey, 82 percent of participating hospital information security leaders reported having a significant security incident in the last 12 months, with a majority of these known incidents being caused by "bad actors" such as cybercriminals.[12] "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[13]

28. As a healthcare provider Northwood knew, or should have known, the importance of safeguarding patient PII entrusted to it and of the foreseeable consequences if its data security systems were breached, including the significant

---

[11] *Id.*

[12] https://www.himss.org/2019-himss-cybersecurity-survey (last visited June 14, 2019).

[13] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, available at https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks.

costs that would be imposed on its patients as a result of a breach, yet failed to take adequate cyber-security measures to prevent the Data Breach from occurring.

C. Northwood Acquires, Collects, and Stores Plaintiff's and Class Members' PII

29. Defendant acquires, collects, and stores a massive amount of protected health related information and other personally identifiable data on its provider patients.

30. As a condition of engaging in health services, Northwood requires that these patients entrust them with highly sensitive personal information.

31. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Northwood assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

32. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and the Class Members, as current and former patients, relied on Northwood to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

D. The Value of Personally Identifiable Information and the Effects of Unauthorized Disclosure

33. Northwood was well-aware that the PII it collects is highly sensitive, and of significant value to those who would use it for wrongful purposes.

34. Personally identifiable information is a valuable commodity to identity thieves. As the FTC recognizes, with PII identity thieves can commit an array of crimes including identify theft, medical and financial fraud.[14] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII on multiple underground Internet websites.

35. While credit card information and associated PII can sell for as little as $1-$2 on the black market, protected health information can sell for as much as $363 according to the Infosec Institute. This is because one's personal health history (e.g. ailments, diagnosis, surgeries, etc.) cannot be changed.[15] PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

36. In addition to PHI, the Plaintiff's and Class Members' other PII is also valuable. For example, Social Security numbers are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

---

[14] Federal Trade Commission, *Warning Signs of Identity Theft*, https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft

[15] Center for Internet Security, Data Breaches: In the Healthcare Sector, https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector

37. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

38. Moreover, it is not easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[16]

---

[16] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited February 13, 2019).

39. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[17] As explained above, the inclusion of PHI, such as the information exposed here, is even more valuable.[18]

40. At all relevant times, Northwood knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences if its data security systems were breached, including, the significant costs that would be imposed on patients as a result of a breach.

E. Northwood's Conduct Violates HIPAA

41. The Healthcare Insurance Portability and Accountability Act, 4 U.S.C. § 1320 *et seq.* ("HIPAA"), requires covered entities to protect against reasonably anticipated threats to the security of PHI. Covered entities must implement

---

[17] *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, Feb. 6, 2015, *available at* http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited February 13, 2019).

[18] *Supra* at n. 12.

safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.[19]

42. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendants left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

43. Defendant's Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations. Northwood's security failures include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic protected health information that Defendant creates, receives, maintains, and transmits in violation of 45 CFR §164.306(a)(1);

b. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or

[19] https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/

software programs that have been granted access rights in violation of 45 CFR §164.312(a)(1);

c. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR §164.308(a)(1);

d. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR §164.308(a)(6)(ii);

e. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR §164.306(a)(2);

f. Failing to protect against any reasonably anticipated uses or disclosures of electronically protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR §164.306(a)(3);

g. Failing to ensure compliance with HIPAA security standard rules by their workforce in violation of 45 CFR §164.306(a)(94);

h. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR §164.502, *et seq.*;

i. Failing to effectively train all members of their workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of protected health information in violation of 45 CFR §164.530(b) and 45 CFR §164.308(a)(5); and

j. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 CFR §164.530(c).

F. Northwood's Actions Fail to Comply with FTC Guidelines

44. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable

data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[20]

45. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses.[21] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

46. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for

---

[20] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[21] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[22]

47. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

48. Northwood failed to properly implement basic data security practices. Northwood's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

49. Northwood was at all times fully aware of its obligation to protect the PII of patients because of its position as a trusted healthcare provider. Northwood was also aware of the significant repercussions that would result from its failure to do so.

---

[22] FTC, *Start With Security*, *supra* note 19.

G. Northwood Fails to Comply with Industry Standards

50. Data exfiltrated from healthcare providers continues to be a high value target among cybercriminals. In 2017, the U.S. healthcare sector experienced over 330 data breaches, a number which continued to grow in 2018 (363 breaches).[23] The costs of healthcare data breaches are among the highest across all industries, topping $380 per stolen record in 2017 as compared to the global average of $141 per record. *Id.* As a result, both the government and private sector have developed industry best standards to address this growing problem.

51. The Department of Health and Human Services' Office for Civil Rights ("DHHS") notes that "[w]hile all organizations need to implement policies, procedures, and technical solutions to make it harder for hackers to gain access to their systems and data, this is especially important in the healthcare industry. Hackers are actively targeting healthcare organizations as they store large quantities of highly sensitive and valuable data."[24] DHHS highlights several basic cybersecurity safeguards that can be implemented to improve cyber resilience which require a relatively small financial investment, yet can have a major impact on an

[23] https://www.ntiva.com/blog/10-cybersecurity-best-practices-for-the-healthcare-industry; Identity Theft Resource Center, 2018 End of Year Data Brach Report, https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf

[24] HIPAA Journal, Cybersecurity Best Practices for Healthcare Organizations, https://www.hipaajournal.com/important-cybersecurity-best-practices-for-healthcare-organizations/

organization's cybersecurity posture including: (a) the proper encryption of PII; (b) education and training healthcare employees on how to identify social engineering attacks; (c) reviewing audit logs regularly in order to identify attempts by unauthorized individuals to gain access to PII/PHI before they result in a data breach; and (d) correct the configuration of software and network devices.

52. Private cyber security firms have also identified the healthcare sector as being particularly vulnerable to cyber-attacks, both because of the of value of the PII that it maintains and because, as an industry, it has been slow to adapt and respond to cybersecurity threats.[25] They too have promulgated similar best practices for bolstering cyber security and protecting against the unauthorized disclosure of PII.

53. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry, Northwood chose to ignore them. Only after the Data Breach did Northwood institute and fortify some protections that should have already been in place to prevent incidents such as the Data Breach including: (1) "mandatory password resets for all employee email accounts and notified employees to be on the lookout for suspicious emails;"

[25] See e.g., https://www.ntiva.com/blog/10-cybersecurity-best-practices-for-the-healthcare-industry; https://resources.infosecinstitute.com/category/healthcare-information-security/is-best-practices-for-healthcare/10-best-practices-for-healthcare-security/#gref.

(2) "additional technical safeguards on our email system;" and (3) "training and education for our employees in order to prevent similar future incidents."[26]

54. Each of these preventative measures have long been cornerstones in industry best practices and should have been implements before the Data Breach, not afterwards. These best practices were known, or should have been known by Northwood, whose failure to heed and properly implement them directly led to the Data Breach and the unlawful exposure of PII.

H. Plaintiff and Class Members Suffered Damages

55. The ramifications of Defendant's failure to keep Patients' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[27]

56. The PII belonging to Plaintiff and Class Members is private, sensitive in nature, and was left inadequately protected by Defendants who did not obtain Plaintiff's or Class Members' consent to disclose such PII to any other person as required by applicable law and industry standards.

---

[26] https://northwoodinc.com/notice-of-data-privacy-event.

[27] 2014 LexisNexis True Cost of Fraud Study, https://www.lexisnexis.com/risk/downloads/|assets/true-cost-fraud-2014.pdf.

57. The Data Breach was a direct and proximate result of Northwood's failure to: (a) properly safeguard and protect Plaintiff's and Class Members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' PII; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

58. Defendant had the resources necessary to prevent the Breach, but neglected to adequately invest in data security measures, despite its obligation to protect Patient data.

59. Had Defendant remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, they would have prevented the intrusions into their systems and, ultimately, the theft of PII.

60. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives. The U.S. Department of Justice's Bureau of Justice

Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[28]

61. To date, Northwood has merely offered "access to complimentary credit monitoring services."[29] The offer, however, is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and it entirely fails to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

62. Furthermore, Defendant's credit monitoring offer to Plaintiff and Class Members squarely places the burden on Plaintiff and Class Members, rather than on the Defendant, to investigate and protect themselves from Defendant's tortious acts resulting in the Data Breach. Rather than automatically enrolling Plaintiff and Class Members in credit monitoring services upon discovery of the breach, Defendant merely sent instructions "offering" the services to affected patients recommending they sign up for the services.

---

[28] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013 available at https://www.bjs.gov/content/pub/pdf/vit12.pdf (last visited April 19,2019).

[29] https://www.prnewswire.com/news-releases/northwood-inc-provides-notice-of-data-security-incident-300884252.html

63. As a result of the Defendant's failures to prevent the Data Breach, Plaintiff and Class Members have suffered, will suffer, or are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their PII;

b. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

d. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the PII in their possession; and

e. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair

the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

64. In addition to a remedy for the economic harm, Plaintiff and the Class maintain an undeniable interest in ensuring that their PII is secure, remains secure, and is not subject to further misappropriation and theft.

I. Defendant's Delay in Identifying & Reporting the Data Breach Caused Additional Harm

65. It is axiomatic that "[t]he quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit the damage. Early notification can also help limit the liability of a victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act."[30]

66. Indeed, once a data breach has occurred, "[o]ne thing that does matter is hearing about a data breach quickly. That alerts consumers to keep a tight watch on credit card bills and suspicious emails. It can prompt them to change passwords and freeze credit reports. And notifying officials can help them catch cybercriminals and warn other businesses of emerging dangers. If consumers don't know about a breach

---

[30] *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, Business Wire, https://www.businesswire.com/news/home/20170201005166/en/Identity-Fraud-Hits-Record-High-15.4-Million.

because it wasn't reported, they can't take action to protect themselves" (internal citations omitted).[31]

67. Although the Data Breach occurred on May 3, 2019, and was discovered three days later, Northwood took more thantwo months to notify affected patients, depriving them of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

68. As a result of Northwood's delay in detecting and notifying consumers of the Data Breach, the risk of fraud for Plaintiff and Class Members has been driven even higher.

CLASS ACTION ALLEGATIONS

69. Plaintiff seeks relief on behalf of herself and as representatives of all others who are similarly situated. Pursuant to Fed. R. Civ. P. Rule 23(a), (b)(2), (b)(3) and (c)(4), Plaintiff seeks certification of a Nationwide class defined as follows:

> All persons whose PII was compromised as a result of the Data Breach announced by Northwood on July 12, 2019 (the "Class").

70. Plaintiff also seeks certification of a Michigan state-wide sub-class defined as follows:

---

[31] Consumer Reports, The Data Breach Next Door Security breaches don't just hit giants like Equifax and Marriott. Breaches at small companies put consumers at risk, too, January 31, 2019, https://www.consumerreports.org/data-theft/the-data-breach-next-door/

> All persons who reside in the state of Michigan whose PII was compromised as a result of the Data Breach announced by Northwood on July 12, 2019 (the "Class").

71. Excluded from the Class are Northwood and any of its affiliates, parents or subsidiaries; all persons who make a timely election to be excluded from the Class; government entities; and the judges to whom this case is assigned, their immediate families, and court staff.

72. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

73. The proposed Class meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and (c)(4).

74. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. The Data Breach implicates 15,027 current and former Northwood patients. Northwood has physical and email addresses for Class members who therefore may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

75. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves

common questions of law and fact that predominate over any questions affecting individual Class members. The common questions include:

a. Whether Northwood had a duty to protect patient PII;

b. Whether Northwood knew or should have known of the susceptibility of its systems to a data breach;

c. Whether Northwood's security measures to protect its systems were reasonable in light of best practices recommended by data security experts;

d. Whether Northwood was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether Northwood's failure to implement adequate data security measures allowed the breach of its data systems to occur;

f. Whether Northwood's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the unlawful exposure of the Plaintiff's and Class Members' PII;

g. Whether Plaintiff and Class Members were injured and suffered damages or other losses because of Northwood's failure to reasonably protect its systems and data network; and,

h. Whether Plaintiff and Class members are entitled to relief.

76. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Rule 23(a)(3), Plaintiff's claims are typical of those of other Class members. Plaintiff was a Northwood patient whose PII was exposed in the Data Breach. Plaintiff's damages and injuries are akin to other Class Members, and Plaintiff seeks relief consistent with the relief sought by the Class.

77. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class he seeks to represent; is committed to pursuing this matter against Northwood to obtain relief for the Class; and has no conflicts of interest with the Class. Moreover, Plaintiff's Counsel are competent and experienced in litigating class actions, including privacy litigation of this kind. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

78. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The quintessential purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to an individual plaintiff may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class are relatively small compared to the burden and expense required to individually litigate their claims

against Northwood, and thus, individual litigation to redress Northwood's wrongful conduct would be impracticable. Individual litigation by each Class member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

79. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

80. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Northwood failed to timely notify the public of the Data Breach;

b. Whether Northwood owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Northwood's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard patient PII;

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the data breach; and

g. Whether Northwood filed to comply with its obligations under HIPAA.

81. Finally, all members of the proposed Classes are readily ascertainable. Northwood has access to patient names and addresses affected by the Data Breach. Using this information, Class members can be identified and ascertained for the purpose of providing notice.

FIRST CAUSE OF ACTION
NEGLIGENCE

82. Plaintiff restates and realleges paragraphs 1 through 81 above as if fully set forth herein.

83. As a condition of receiving services, Plaintiff and Class Members were obligated to provide Northwood directly, or through their respective insurance carriers, with their PII.

84. Plaintiff and the Class Members entrusted their PII to Northwood with the understanding that Northwood would safeguard their information.

85. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

86. Defendant had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining and testing the Defendants' security protocols to ensure that PII in its possession was adequately secured and protected and that employees tasked with maintaining such information were adequately training on cyber security measures regarding the security of such information.

87. Plaintiff and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew of or

should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, the current cyber scams being perpetrated and that it had inadequate employee training and education and IT security protocols in place to secure the PII of Plaintiff and the Class.

88. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decision not to comply with HIPAA and industry standards for the safekeeping and encrypted authorized disclosure of the PII of Plaintiff and Class Members.

89. Plaintiff and the Class Members had no ability to protect their PII that was in Northwood's possession.

90. Defendants were in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

91. Defendant had a duty to put proper procedures in place in order to prevent the unauthorized dissemination Plaintiff and Class Members' PII.

92. Defendant has admitted that Plaintiff's and Class Members' PII was wrongfully disclosed to unauthorized third persons as a result of the Data Breach.

93. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding the Plaintiff's and Class Members' PII while it was within the Northwood's possession or control.

94. Defendant improperly and inadequately safeguarded Plaintiff's and Class Members' PII in deviation of standard industry rules, regulations and practices at the time of the Data Breach.

95. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its patients' PII.

96. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately disclose to Plaintiff and Class Members the existence, and scope of the Data Breach.

97. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class Members, Plaintiff's and Class Members' PII would not have been compromised.

98. There is a temporal and close causal connection between Defendant's failure to implement security measures to protect the PII and the harm suffered, or risk of imminent harm suffered by Plaintiff and the Class.

99. As a result of Defendant's negligence, Plaintiff and the Class Members have suffered and will continue to suffer damages and injury including, but not limited to: out-of-pocket expenses associated with procuring robust identity protection and restoration services; increased risk of future identity theft and fraud, the costs associated therewith; time spent monitoring, addressing and correcting the current and future consequences of the Data Breach; and the necessity to engage legal counsel and incur attorneys' fees, costs and expenses.

SECOND CAUSE OF ACTION
NEGLIGENCE PER SE

100. Plaintiff restates and realleges Paragraphs 1 through 81 above as if fully set forth herein.

101. Violation of statute which establishes a duty to take precautions to protect a particular class of persons from a particular injury or type of injury may constitute negligence per se.

102. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Northwood, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

103. Northwood violated Section 5 of the FTC Act by failing to use reasonable measures to protect patient PII and not complying with applicable

industry standards, as described in detail herein. Northwood's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiff and Class Members.

104. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

105. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

106. Based upon the conduct alleged herein, Northwood's violation of Section 5 of the FTC Act constitutes negligence per se.

107. As a direct and proximate result of Northwood's negligence per se, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from the Data Breach including, but not limited to: damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial and medical accounts, closely reviewing and monitoring their credit reports and various

accounts for unauthorized activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect.

108. Additionally, as a direct and proximate result of Northwood's negligence per se, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remains in Northwood's possession and is subject to further unauthorized disclosures so long as Northwood fail to undertake appropriate and adequate measures to protect the PII in its continued possession.

THIRD CAUSE OF ACTION
INVASION OF PRIVACY

109. Plaintiff restates and realleges paragraphs 1 through 81 above as if fully set forth herein.

110. Plaintiff and Class Members had a legitimate expectation of privacy with respect to their PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

111. Defendant owed a duty to patients in its network, including Plaintiff and Class Members, to keep their PII confidential.

112. The unauthorized release of PII, especially the type related to personal health information, is highly offensive to a reasonable person.

113. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their PII to Defendant

as part of their use of Northwood's services, but privately, with the intention that the PII would be kept confidential and protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

114. The Data Breach constitutes an intentional interference with Plaintiff and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

115. Defendant acted with a knowing state of mind when they permitted the Data Breach because it knew its information security practices were inadequate.

116. Acting with knowledge, Northwood had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and Class Members.

117. As a proximate result of Defendant's acts and omissions, Plaintiff's and Class Members' PII was disclosed to and used by third parties without authorization, causing Plaintiff and Class Members to suffer damages.

118. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons.

119. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

FOURTH CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT

120. Plaintiff restates and realleges paragraphs 1 through 81 above as if fully set forth herein.

121. Plaintiff and Class Members were required to provide their PII, including their names, addresses, dates of birth, Social Security numbers, driver's license numbers and various health related information to Defendant as a condition of their use of Defendant's services.

122. Plaintiff and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services, along with Defendant's promise to protect their health information and other PII from unauthorized disclosure.

123. In their written privacy policies, Northwood expressly promised Plaintiff and Class Members that they would only disclose protected health information and other PII under certain circumstances, none of which relate to the Data Breach.

124. Northwood promised to comply with HIPAA standards and to make sure that Plaintiff's and Class Members' health information and other PII would remain protected.

125. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide protected health information and other PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) to prevent unauthorized disclosures of the PII, (d) to provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) to reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, (f) to retain the PII only under conditions that kept such information secure and confidential.

126. Without such implied contracts, Plaintiff and Class Members would not have provided their PII to Defendant.

127. Plaintiff and Class Members fully performed their obligations under the implied contract with Defendant, however, Defendant did not.

128. Defendant breached the implied contracts with Plaintiff and Class Members by failing to:

a. reasonably safeguard and protect Plaintiff and Class Members' PII, which was compromised as a result of the Data Breach.

b. comply with their promise to abide by HIPAA.

c. ensure the confidentiality and integrity of electronic protected health information Defendant created, received, maintained, and transmitted in violation of 45 C.F.R. § 164.306(a)(1).

d. implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1).

e. implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1).

f. identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii).

g. to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. § 164.306(a)(2).

FIFTH CAUSE OF ACTION
UNJUST ENRICHMENT

129. Plaintiff restates and realleges paragraphs 1 through 81 above as if fully set forth herein.

130. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and in so doing provided Defendant with their PII. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their PII protected with adequate data security.

131. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

132. The amounts Plaintiff and Class Members paid for goods and services were used, in part, to pay for use of Defendant's network and the administrative costs of data management and security.

133. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

134. Defendant failed to secure Plaintiff's and Class Members' PII and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

135. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

136. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to Defendant's services.

137. Plaintiff and Class Members have no adequate remedy at law.

138. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in their continued possession; and (vi) future costs in terms of time, effort, and money

that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

139. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

140. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

SIXTH CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY

141. Plaintiff restates and realleges paragraphs 1 through 81 above as if fully set forth herein.

142. In light of their special relationship, Defendant has become the guardian of Plaintiff and Class Member's PII. Defendant has become a fiduciary, created by its undertaking and guardianship of patient PII, to act primarily for the benefit of its patients, including Plaintiff and Class Members. This duty included the obligation to safeguard Plaintiff and Class Member PII and to timely notify them in the event of a data breach.

143. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its relationship. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to:

a. properly encrypt and otherwise protect the integrity of the system containing Plaintiff's and Class Members' protected health information and other PII;

b. timely notify and/or warn Plaintiff and Class Members of the Data Breach.

c. ensure the confidentiality and integrity of electronic protected health information Defendants created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d. implement technical policies and procedures to limit access to only those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

e. implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1);

f. to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security

incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

g. to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. § 164.306(a)(2);

h. to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

i. ensure compliance with the HIPAA security standard rules by their workforce in violation of 45 C.F.R. § 164.306(a)(94).

j. improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, et seq.;

k. effectively train all members of their workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of protected health information

in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5).

l. design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R. § 164.530(c).

m. otherwise failing to safeguard Plaintiff's and Class Members' PII.

144. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Patient PII in their continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the

impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

145. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

SEVENTH CAUSE OF ACTION
MICHIGAN CONSUMER PROTECTION ACT,
Mich. Comp. Laws Ann. §§ 445.903, *et seq.*
(Asserted by the Michigan Subclass)

146. Plaintiff restates and realleges paragraphs 1 through 81 above as if fully set forth herein.

147. Northwood, operating in Michigan, engaged in unfair, unconscionable, and deceptive methods, acts, and practices in the conduct of trade and commerce, including representing that its good and services had characteristics that they did not, representing that its goods and services were of a particular standard when they were not, and advertising its goods and services with intent not to dispose of them as advertised, in violation of Mich. Comp. Laws Ann. § 445.903(1). This includes but is not limited to the following:

a. Failing to enact adequate privacy and security measures to protect Michigan Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. Failing to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Knowingly and fraudulently misrepresenting that it would maintain adequate data privacy and security practices and procedures to safeguard Michigan Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;

d. Omitting, suppressing, and concealing the material fact of the inadequacy of its privacy and security protections for Michigan Subclass Members' PII;

e. Knowingly and fraudulently misrepresenting that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Michigan Subclass Members' PII;

f. Failing to maintain the privacy and security of Michigan Subclass Members' Personal Information, in violation of duties imposed by applicable federal and state laws;

g. Failing to disclose the Data Breach to Michigan Subclass Members in a timely and accurate manner, in violation of the duties imposed by Mich. Comp. Laws Ann. § 445.72(1).

148. As a direct and proximate result of these practices, Michigan Subclass Members suffered injuries to legally protected interests, as described above, including but not limited to their legally protected interest in the confidentiality and privacy of their Personal Information, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their PII.

149. The above unfair and deceptive practices and acts by Northwood were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Michigan Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition. These acts were within the penumbra of common law, statutory, or other established concepts of unfairness.

150. Northwood knew or should have known that its computer systems and data security practices were inadequate to safeguard Michigan Subclass Members' PII and that risk of a data breach or theft was high. Northwood's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and

willful, and/or wanton and reckless with respect to the rights of Michigan Subclass Members.

151. Plaintiff and Michigan Subclass Members seek injunctive relief to enjoin Northwood from continuing its unfair and deceptive acts; monetary relief against Northwood measured as the greater of (a) actual damages in an amount to be determined at trial and (b) statutory damages in the amount of $250 for Plaintiff and each Michigan Subclass Member; reasonable attorneys' fees; and any other just and proper relief available under Mich. Comp. Laws Ann. § 445.911.

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, respectfully requests the following relief:

a. An Order certifying this case as a class action;

b. An Order appointing Plaintiff as the class representative;

c. An Order appointing undersigned counsel as class counsel;

d. A mandatory injunction directing the Defendants to hereinafter adequately safeguard the PII of the Class by implementing improved security procedures and measures;

e. An award of damages;

f. An award of costs and expenses;

g. An award of attorneys' fees; and

h. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial as to all issues triable by a jury.

.

Dated: October 7, 2019

Respectfully submitted,

/s/ *Michael N. Hanna*
Michael N. Hanna (P81462)
MORGAN & MORGAN, P.A.
2000 Town Center,
Suite 1900
Southfield, MI 48075
(313) 251-1399
mhanna@forthepeople.com

Jean Sutton Martin
Ryan J. McGee
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 559-4908
jeanmartin@forthepeople.com
rmcgee@forthepeople.com

Counsel for Plaintiffs